2004pc922

84

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 513 061 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.03.2005 Bulletin 2005/10

(51) Int Cl.7: **G06F 7/58**

(21) Application number: **03020077.8**

(22) Date of filing: **04.09.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(71) Applicant: **Infineon Technologies AG**
81669 München (DE)

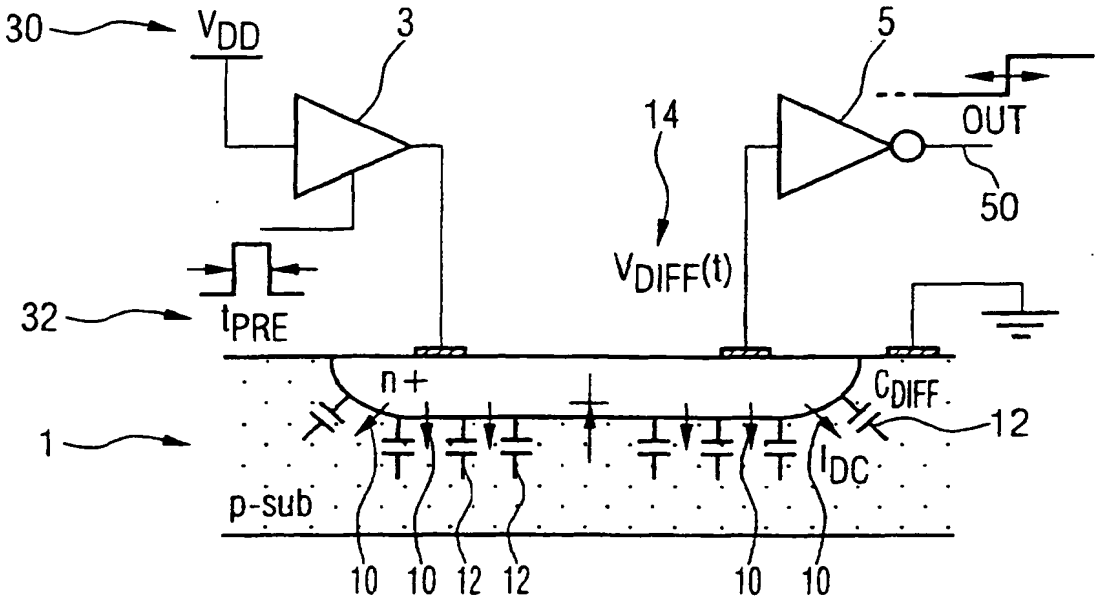
(72) Inventor: **Luzzi, Raimondo, Dr.**
8020 Graz (AT)

(74) Representative: **Schoppe, Fritz, Dipl.-Ing. et al**
Patentanwälte
Schoppe, Zimmermann, Stöckeler & Zinkler
Postfach 246
82043 Pullach bei München (DE)

(54) Apparatus for providing a jittered clock signal and for providing random bits

(57) An apparatus for providing a jittered clock signal comprises a reverse-biased diode (1). The reversed-biased diode (1) comprises a leakage current (10) which decreases a reverse voltage (14) on the diode, time-dependent on a shot-noise of the leakage current. The apparatus for providing a jittered clock signal further comprises means (3) for periodically increasing the reverse voltage of the diode to a value (30), which is above a switching value and the apparatus comprises means (5) for comparing the reverse voltage of the diode (1) to the switching value and for outputting a jittered clock signal (50) dependent on the comparison.

FIG 1



EP 1 513 061 A1

Description

[0001] The present invention relates to an apparatus for providing a jittered clock signal and to an apparatus for providing a random bit and, in particular, to an apparatus for providing a jittered clock signal and an apparatus for providing a random bit, which comprise a diode.

[0002] The expanding field of digital communication requires solutions for securing data which is stored and transferred to and from a digital communication system. Cryptographic algorithms that require a high quality random number source are widely used in communication systems and especially in Smart Cards. Random numbers are used for secret keys, signatures, authentication protocols, padding bytes or blinding values. Typically, a Smart Card micro-controller features a truly random number generator among its peripheral devices. Even modern motherboards or PCs comprise a security device, which includes a random number generator.

[0003] According to the prior art, direct amplification of a noise source from a non-deterministic natural source, like electronic noise or radioactive decay, jittered oscillator sampling and discrete-time chaotic maps are widely exploited for generating a random stream. Such techniques are often combined in order to improve a near-random behaviour of a particular random stream generating technique.

[0004] The paper "A high-speed oscillator-based truly random number generator", M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, M. Varanonuovo, IEEE Trans. Computers, Vol. 52, No. 4, pp. 403-409, April 2003 describes a truly random number generator which exploits the jittered oscillator technique, where a sampling oscillator is provided with an amplified noise source in order to achieve a high jitter to mean period ratio.

[0005] The paper "A high-speed truly IC random number of source for Smart Card microcontrollers", M. Bucci, L. Germani, R. Luzzi, P. Tommasino, A. Trifiletti, M. Varanonuovo, Proc. 9th IEEE International Conf. On Electronics, Circuits and Systems (ICECS 2002), pp. 239-242, Sept. 2002 presents a design of a very high-speed thermal noise-based mixed-signal random number generator, which features a near-random behaviour for clock frequencies up to 80 MHz. The proposed random number generator is based on an amplification of thermal noise from integrated resistors. The amplified noise is compared to a reference voltage by a clocked comparator whose output is random bit-streamed.

[0006] The noise-based random number generation technique is the most popular technique for generating a random stream. Nevertheless, the lack of adequate shielding from power supply and substrate signals in an integrated circuit environment prohibits the exclusive use of this method for integrated circuit-based cryptographic systems. Published random number generator designs using ring oscillators report that typical levels of oscillator jitter are not nearly sufficient to produce statistical randomness. Consequently, pseudo-random techniques are added to further randomise the output. The same is true for discrete-time chaos systems that can be electronically implemented using discrete-time analogue signal processing techniques.

[0007] Therefore, the paper "A noise-based IC random number generator for applications in cryptography", C.S. Petrie, J.A. Connelly, IEEE Trans. Circuits and Systems I, Vol. 47, No. 5, pp. 615-621, May 2000 proposes a combination of direct amplification, oscillator sampling and discrete-time chaos, for a random number generating system. Amplified thermal noise is summed into an analogue-digital-based chaotic system that is used to drive a current-controlled oscillator. The current-controlled-oscillator output is assembled at a lower, user-defined clock frequency using a data flip-flop. Due to the combination of three techniques for generating a random stream, the architecture is very complex.

[0008] It is the object of the present invention to provide a cost-effective, low area and power requiring apparatus for providing a true deterministic jittered clock signal and an apparatus for providing a random bit.

[0009] This object is achieved by an apparatus for providing a digital clock signal according to claim 1 and an apparatus for providing a random bit according to claim 7.

[0010] The present invention provides an apparatus for providing a jittered clock signal, comprising:

a reverse-biased diode, wherein the diode comprises a leakage current which decreases a reverse voltage on the diode, time-dependent on a shot-noise of the leakage current;

means for periodically increasing the reverse voltage of the diode to a value which is above a switching value, and

means for comparing the reverse voltage of the diode to the switching value and for outputting a clock signal dependent on the comparison.

[0011] The present invention further provides an apparatus for providing a random bit comprising:

a first apparatus for providing a first jittered clock signal and a second apparatus for providing a second jittered clock signal; and
means for comparing the first and the second clock signal and for outputting a random bit dependent on a result of the comparison.

[0012] The present invention is based on the finding that a shot-noise of a leakage current of a reverse-biased diode can be advantageously used for generating a jittered clock signal.

[0013] According to the inventive arrangement, the reverse-biased diode is supplied with an input signal

that periodically increases the reverse voltage of the diode. Due to its characteristic, the apparatus for providing a jittered clock signal generates a jittered output signal from the periodic input signal.

[0014] The paper "Analysis of temporal noise in CMOS photodiode active pixel sensor", H. Tian, B. Fowler, A. El Gamal, IEEE J. Solid-State Circuits, Vol. 36. No. 1, pp. 92-101, Jan. 2001 presents an analysis of a photodiode shot noise.

[0015] According to a preferred embodiment of the present invention, two apparatus for providing a jittered clock signal are combined for providing an apparatus for providing a random bit. A true random bit stream is obtained by comparing the jittered clock signal outputs of the first and the second apparatus for providing a jittered clock signal outputting a random bit based on the comparison.

[0016] The inventive arrangement offers a very low power dissipation, a low area requirement in an integrated circuit and an easy portability within different designs, as no analogue circuits are employed. Moreover, a symmetrical layout is possible for the apparatus for providing a random bit, thus avoiding a sensibility to deterministic disturbances. In an embodiment which comprises a plurality of jittered clock signals, the high jitter level of the jittered clock signals prevents a synchronisation of the different jittered clock signals due to power supply and substrate couplings.

[0017] Preferred embodiments of the present invention are described hereinafter, making reference to the appended drawings:

Fig. 1 shows a schematic view of an apparatus for providing a jittered clock signal according to the present invention;

Fig. 2 shows a characteristic decrease of a reverse voltage of an apparatus for providing a jittered clock signal according to a preferred embodiment of the present invention;

Fig. 3 shows a schematic view of an apparatus for providing a random bit according to a preferred embodiment of the present invention;

Fig. 4 shows a further embodiment of an apparatus for providing a random bit;

Fig. 5 shows a schematic view of the decrease of a reverse voltage of an apparatus for providing a jittered clock signal; and

Fig. 6 shows a further embodiment of an apparatus for providing an additional random bit.

[0018] Fig. 1 shows an apparatus for providing a jittered clock signal according to a preferred embodiment of the present invention. The apparatus for providing a jittered clock signal comprises a reverse-biased diode 1, means 3 for periodically increasing a reverse voltage of the diode 1 and means 5 for comparing the reverse voltage of the diode 1 to a switching value and for outputting a clock signal depending on the comparison.

[0019] In this embodiment, the diode 1 is a reverse-biased P-N junction, like an n/n+ resistance diffused into the p-type substrate. The means 3 for periodically increasing a reverse voltage of the diode 1 is a tri-state buffer and the means 5 for comparing a reverse voltage of the diode 1 to a threshold voltage and for outputting a clock signal depending on the comparison is a CMOS inverter.

[0020] The depletion region A_{DIFF} of the diode 1, comprises a leakage current or dark current I_{DC} 10 due to thermally generated minority carriers. A shot noise $I_{DC}(t)$ is associated to such a leakage current 10. The depletion region of the reverse biased diode 1 offers a capacitance C_{DIFF} 12. The tri-state buffer 3 charges a reverse voltage $V_{DIFF}(t)$14 of the capacitance C_{DIFF} 12 by connecting the diode 1 to a supply voltage V_{DD} 30. When the tri-state buffer 3 is tri-stated, the capacitance C_{DIFF} 12 discharges due to the current I_{DC} 10. During the discharge time, the shot noise $I_{DC}(t)$ of the current I_{DC} 10 is integrated by the capacitance C_{DIFF} 12, thus obtaining a variance for the reverse voltage $V_{DIFF}(t)$14 which represents a diffusion voltage of the diode 1. The inverter 5 is connected to the depletion region of the diode 1 and compares the reverse voltage $V_{DIFF}(t)$ 14 to a threshold voltage V_{TH}. The inverter 5 outputs an output signal 50 which depends on the time, it takes the reverse voltage $V_{DIFF}(t)$ 14 to decrease from the supply voltage V_{DD} 30 to the threshold voltage V_{TH}. Thus, a switching time of the output signal 50 depends on a random variable due to the shot noise $I_{DC}(t)$.

As the tri-state buffer 3 periodically increases the reverse voltage $V_{DIFF}(t)$ 14, the output signal 50 is a jittered clock signal 50.

[0021] Fig. 2 shows characteristic decreases of a diffusion voltage $V_{DIFF}(t)$ 214 in an apparatus for providing a jittered clock signal as it is shown in Fig. 1. During the time period 236 the diffusion voltage $V_{DIFF}(t)$ 214 decreases due to a leakage current I_{DC}. Further, Fig. 2 shows a jittered clock signal 250 as it is outputted from the apparatus for providing a jittered clock signal.

[0022] A first characteristic 214a shows an idealized decrease of the diffusion voltage $V_{DIFF}(t)$ 214 from the supply voltage 230 due to the leakage current I_{DC} if there is no shot noise $I_{DC}(t)$. When the diffusion voltage $V_{DIFF}(t)$ 214 decreases to a threshold voltage V_{TH} 252 the output clock signal 250 is switched 254. As a realistic leakage current I_{DC} of a diode comprises a shot noise $I_{DC}(t)$, realistic characteristics 214b, c, d differ from the theoretical characteristic 214a. Thus, the decrease of the diffusion voltage $V_{DIFF}(t)$ 214 can be faster (214c, 214d) or slower (214b) than the theoretical decrease 214a. Therefore, the diffusion voltage $V_{DIFF}(t)$ 214 decreases to the threshold voltage V_{TH} 252 not in a fixed

time period, but after a time period that includes a random variable. Thus, the switching time 254 of the output clock signal 250 depends on the random variable which is responsible for the jitter of the output clock signal 250.

[0023] According to a further embodiment, a variance of the switching time 254 is exploited to generate a random bit. Fig. 3 shows a schematic view of an apparatus for providing a random bit based on the jittered output clock signal of an apparatus for providing a jittered clock signal.

[0024] Fig. 3 shows an apparatus for providing a random bit, which comprises a first apparatus 300a for providing a jittered clock signal and a second apparatus 300b for providing a jittered clock signal. As described in Fig. 1, each apparatus 300a, b comprises a reverse-biased diode 301, a tri-state buffer 303 and an inverter 305. The diode 301 comprises a leakage current I_{DC} 310. A supply voltage V_{DD} 330 is applied to the diodes 301, while the tri-state buffers 303 are in an active state. The tri-state buffers 303 switch according to a periodic reset signal 334. Each apparatus for providing a jittered clock signal 300a, b outputs an jittered clock signal 350a, 350b. As described in Fig. 2 each jittered clock signal 350a, 350b comprises a random switching characteristic. Thus, a switching time of the jittered clock signals 350a, b varies around a mean switching time.

[0025] The two jittered clock signals 350a, b are taken as an input to a sampling circuit 360. In this embodiment, the sampling circuit 360 is a digital flip-flop. The first jittered clock signal 350a is connected to the data input of the digital flip-flop 360 and the second jittered clock signal 350b is connected to the clock input of the digital flip-flop 360. Thus, the second jittered clock signal 350b is used to sample the first jittered clock signal 350a. The sampled first jittered clock signal 350a is outputted by the digital flip-flop 360 as a random bit 362.

[0026] The value of the random bit depends on the switching times of the jittered clock signals 350a, b. In order to generate a true random bit stream 362, the mean switching time values of the jittered clock signals 350a, b have to be aligned. Although the apparatus for providing a random bit comprises two nominally-identical apparatus 300a, b for providing a jittered clock signal, the two mean switching time values are different due to matching errors over the diffusion regions, driver-disable times, inverter thresholds, inverter communication times and inter-connection delays. In the embodiment shown in Fig. 3, the mean switching time of the first apparatus 300a is smaller than the mean switching time of the second apparatus 300b, resulting in an unbalanced bit stream of the random bits 362.

[0027] In order to avoid the time difference 356 of the switching times of the two jittered clock signals 350a, b which causes an unbalanced bit stream of the random bits 362, an alignment of the mean switching times is to be controlled by a feedback loop, as it is shown in the embodiment of an apparatus for providing a random bit in Fig. 4.

[0028] According to the embodiment shown in Fig. 3, the embodiment shown in Fig. 4 comprises a first apparatus 400a and a second apparatus 400b for providing a jittered clock signal which are supplied by a supply voltage 430 which is controlled by a reset signal 434. A first and a second jittered clock signal 450a, b are outputted by the two apparatus 300a, b for providing a jittered clock signal.

[0029] The jittered clock signals 450a, b are not directly connected to a flip-flop 460, which outputs a random bit 462, but to means for aligning a mean switching time of the jittered clock signal 450a to a mean switching time of the second jittered clock signal 450b. The means for aligning comprise means for delaying 470a, b of the jittered clock signals 450a, b and a counter 472. The first means for delaying 470a is connected to the first jittered clock signal 450a and outputs a first delayed clock signal 474a. The second means for delaying 470b is connected to the second jittered clock signal 450b and outputs a second delayed jittered clock signal 474b. The delayed clock signals 474a, b are connected to the flip-flop 460. The random bit 462 is outputted by the flip-flop 460 by way of sampling the first delayed clock signal 474a by the second delayed clock signal 474b. The counter 472 is an up/down counter which counts an counting value up or down depending on the value of the random bit 462. Therefore, the counter 472 takes the random bit 462 as an input. The counter 472 is triggered by the second delayed clock signal 474b. Depending on the counting value, the counter 472 sets 476 a delay time of the second means for delaying 470b. Furthermore, the second delayed clock signal 474b is used to control the reset signal 434, which controls the state of the tri-state buffers of the apparatus 300a, b for providing a jittered clock signal.

[0030] Thus, a feedback loop is realized in order to align the mean switching times of the first and the second jittered clock signals 350a, b. The first jittered clock signal 450a is delayed by the first means for delaying 470a by a time $\Delta T_1=(T_2-T_1)/2$, whereas the second jittered clock signal 450b is delayed by the second means for delaying 470b by a time delay $\Delta T_2 \in [T_1, T_2]$. The time delay ΔT_2 is a variable delay according to the setting output 476 of the counter 472. The counter 472 is used to estimate a mean value of the random bits 362. A precision much smaller than the available jitter of the jittered clock signals 450a, b is required to adjust the delay ΔT_2. The exact value of the delay ΔT_2 is obtained from a biasing error that can be tolerated on a mean value of the random bit 362 stream.

[0031] Once a random bit 462 has been generated, triggered by a rising edge of the second delayed clock signal 474b, a new reset pulse on the reset signal 434 is required to charge again the diffusion capacitances of the diodes of the first and the second apparatus 400a, 400b for providing a jittered clock signal. Thus, the second delayed clock signal 474b is used to trigger reset pulses on the reset signal 434, thus obtaining a contin-

uous operation of the apparatus for providing a random bit.

[0032] Due to the symmetric arrangement of the two apparatus 400a, b for providing a jittered clock signal, common-mode disturbances do not affect the random bit output 462 if a symmetrical layout for the arrangement and, in particular, an inter-digitated layout for the N+ diffusions is used.

[0033] A further advantage of the feedback loop is a compensation of the leakage current values which comprise a variation over process and temperature.

[0034] Fig. 5 shows a schematic characteristic of the diffusion voltage $V_{DIFF}(t)$ 514 over a time period 536, as it is shown in Fig. 2. Fig. 5 illustrates a jitter around a mean switching time of a jittered clock signal of an apparatus for providing a jittered clock signal. The switching time corresponds to a mean integration time which is the time, the diffusion voltage $V_{DIFF}(t)$ 514 needs to decrease from the supply voltage V_{DD} down to the threshold voltage V_{TH}.

[0035] A data-rate of the random BIT stream, generated by an apparatus for providing a random bit is fixed by a mean integration time:

$$\overline{t_{INT_1}} \cong \overline{t_{INT_2}} = \overline{t_{INT}} = \frac{V_{DD} - V_{TH}}{\frac{I_{DC}}{C_{DIFF}}} \qquad (1)$$

[0036] Since both, leakage current I_{DC} and capacitance C_{DIFF} of the depletion region are directly proportional to a diffusion area A_{DIFF}, which defines the boundary of the p/n substrate, the voltage difference $V_{DD} - V_{TH}$ is the only parameter that can be used to change the data-rate of the random BIT stream.

[0037] For the variance of the diffusion voltage V_{DIFF} (t) 514 at the end of the integration time it holds:

$$\sigma^2 V_{DIFF} = \frac{qI_{DC}}{C_{DIFF}^2} t_{INT} \qquad (2)$$

where $q=1.6\times10^{-19}$ C is the electron charge.

[0038] Being $\overline{t_{INT}} >> \sigma_{tINT}$ from equation (2) it follows:

$$\sigma_{VDIFF}^2 \cong \frac{qI_{DC}}{C_{DIFF}^2} \overline{t_{INT}} \qquad (3)$$

[0039] As shown in Figure 5, the integration time has a non-symmetrical probability distribution and it holds:

$$t_{INT}^{+3\sigma} - \overline{t_{INT}} = \frac{3\sigma_{V_{DIFF}}}{V_{DD} - V_{TH} - 3\sigma_{V_{DIFF}}} \overline{t_{INT}} \qquad (4)$$

$$\overline{t_{INT}} - t_{INT}^{-3\sigma} = \frac{3\sigma_{V_{DIFF}}}{V_{DD} - V_{TH} + 3\sigma_{V_{DIFF}}} \overline{t_{INT}} \qquad (5)$$

[0040] However, being $\sigma V_{DIFF} << V_{DD}-V_{TH}$, it follows:

$$t_{INT}^{+3\sigma} - \overline{t_{INT}} \cong \overline{t_{INT}} - t_{INT}^{-3\sigma} = jitter \qquad (6)$$

where,

$$jitter = \frac{3\sigma_{V_{DIFF}}}{V_{DD} - V_{TH}} \overline{t_{INT}} \qquad (7)$$

[0041] From equations (1), (3) and (7), it follows:

$$jitter = 3 \frac{\sqrt{C_{DIFF}}}{I_{DC}} \sqrt{q} \sqrt{V_{DD} - V_{TH}}.$$

[0042] In the present embodiment, the power supply V_{DD} is 1.2 V, the Inverter threshold V_{TH} is 0.8 V, the diffusion area A_{DIFF} is 100 μm^2, the depletion capacitance C_{DIFF} is 0.84fF/μm^2 and the leakage current I_{DC} is 0.4 pA/μm^2.

[0043] Using the above mentioned values it holds:

$$\overline{t_{INT}} = 0.84\,ms$$

$$jitter = 5.5\,\mu s$$

and a data-rate of about 1.2kb/s $(1/\overline{t_{INT}})$ is expected.

[0044] If the obtained data-rate of the apparatus for providing a random bit is too low for a target application, the high jitter level on the delayed clock signals of the embodiment shown in Fig. 4 can be exploited to generate additional random bits for each cycle.

[0045] Such an arrangement for generating more random bits is shown in Fig. 6. The arrangement can be arranged in parallel to the flip-flop shown in Fig. 4. The arrangement comprises an XOR gate 660, a counter 664 and an output register 665 for outputting additional random bits 666. The XOR gate 660 is connected to a first and second delayed clock signal 674a, b. The delayed clock signals 674a, b, which are an input to the XOR gate 660 are outputted by the means for delaying, as can be seen in Fig. 4.

[0046] A compared signal 677 is the result of the XOR combination of the two delayed clock signals 674a, b. A resulting pulse 677' depends on the switching times of the delayed clock signals 674a, b and, therefore has a random duration. The random duration is quantified by the counter 664 which comprises a clock input 678 on which a clock is supplied. The counter 664 counts the number of clock cycles in which the compared signal

677 is active. Triggered by an active value of the compared signal 677, the output register 665 outputs the additional random bit 666. The value of the random bit 666 depends on the value of the counter 664.

[0047] Also, the present invention has been described above, making reference to tri-state buffers, p/n diodes and inverters, it is clear that the present invention is not limited by the shown embodiments. Instead of a tri-state buffer, any means for periodically charging the capacitance of the diode can be used. Instead of the inverter, any means can be used which compares the diffusion voltage of the diode to a threshold voltage and provides a signal that switches accordingly. Moreover, instead of the digital flip-flop and the XOR gate, any means can be used which provides an output bit depending on a comparison between two jittered clock input signals.

List of Reference Numbers

[0048]

1	Diode
3	Tri-state buffer
5	Inverter
10	Leakage current
12	Capacitance of the depletion region
14	Diffusion voltage
30	Supply voltage
32	Signal for controlling the tri-state buffer
50	Jittered clock signal
214	Diffusion voltage
230	Supply voltage
236	Tri-state time period
250	Jittered clock signal
252	Threshold voltage
254	Switching time
214a	First characteristic
214b,c,d	Second, third, fourth characteristics
300a	First apparatus for providing a jittered clock signal
300b	Second apparatus for providing a jittered clock signal
301	Diodes
303	Tri-state buffers
305	Inverters
310	Leakage currents
330	Supply voltage
334	Reset signal
350a, b	Jittered clock signals
346	Time difference of the switching time
360	Data flip-flop
362	Random bit
400a	First apparatus for providing a jittered clock signal
400b	Second apparatus for providing a jittered clock signal
430	Supply voltage
434	Reset signal
450a	First jittered clock signal
450b	Second jittered clock signal
460	Data flip-flop
462	Random bit
470a	First means for delaying
470b	Second means for delaying
472	Counter
474a	First delayed clock signal
474b	Second delayed clock signal
476	Set the second delayed time
514	Diffusion voltage
536	Time period
660	XOR gate
664	Counter
665	Output register
666	Addition random bit
674a, b	Delayed clock signals
677	Compared signals
678	Clock

Claims

1. Apparatus for providing a jittered clock signal (50; 250), comprising:

   a reverse-biased diode (1), wherein the diode comprises a leakage current (10) which decreases a reverse voltage (14) on the diode, time-dependent on a shot-noise of the leakage current;

   means (3) for periodically increasing the reverse voltage of the diode to a voltage (30; 230) which is above a switching value (252); and

   means (5) for comparing the reverse voltage of the diode to the switching value and for outputting a jittered clock signal dependant on the comparison.

2. Apparatus for providing a jittered clock signal according to claim 1, wherein the means (3) for periodically increasing the reverse voltage provides an input clock signal (32) to the diode (1), wherein the input clock signal comprises an active state and a tri-state state, wherein the active state provides a supply voltage (30; 230) with a supply voltage value being above the switching value (252), and wherein the active state is periodically interrupted by the tri-state state for a discharge time period (236) in which the reverse voltage (14; 214) of the diode decreases from the supply voltage value to below the switching value.

3. Apparatus for providing a jittered clock signal according to one of claims 1 or 2, wherein the means for periodically increasing the reverse voltage is

connected to the outputted clock signal and the period in which the reverse voltage is increased depends on the outputted clock signal.

4. Apparatus for providing a jittered clock signal according to one of claims 1 to 3, wherein the means (3) for periodically increasing the reverse voltage of the diode is a tri-state buffer.

5. Apparatus for providing a jittered clock signal according to one of claims 1 to 4, wherein the reverse-biased diode (1) is a reversed-biased P-N junction.

6. Apparatus for providing a jittered clock signal according to one of claims 1 to 5, wherein the means (5) for comparing the reverse voltage to the switching value and for outputting a jittered clock signal is an inverter that is connected to the diode.

7. Apparatus for providing a random bit comprising:

a first apparatus (300a; 400a) for providing a first jittered clock signal (350a; 450a) according to one of claims 1 to 6, and a second apparatus (300b, 400b) for providing a second jittered clock signal (350b; 450b) according to one of claims 1 to 6; and

means (360; 460; 660) for comparing the first and the second clock signal and for outputting a random bit (362. 462) dependent on a result of the comparison.

8. Apparatus for providing a random bit according to claim 7, comprising means (470a, 470b, 472) for aligning a mean switching time of the first jittered clock signal (450a) to a mean switching time of the second jittered clock signal (450b) and for providing a first (474a) and a second (474b) delayed jittered clock signal to the means (460) for comparing.

9. Apparatus for providing a random bit according to one of claims 7 or 8, wherein the means (360; 460) for comparing and for outputting is a D-flip-flop.

10. Apparatus for providing a random bit according to one of claims 7 to 9, wherein the means (660) for comparing further comprises an XOR gate, and wherein an additional random bit (666) is provided dependent on a time delay (677') between edges of the first (674a) and the second (674b) jittered clock signal.

FIG 1

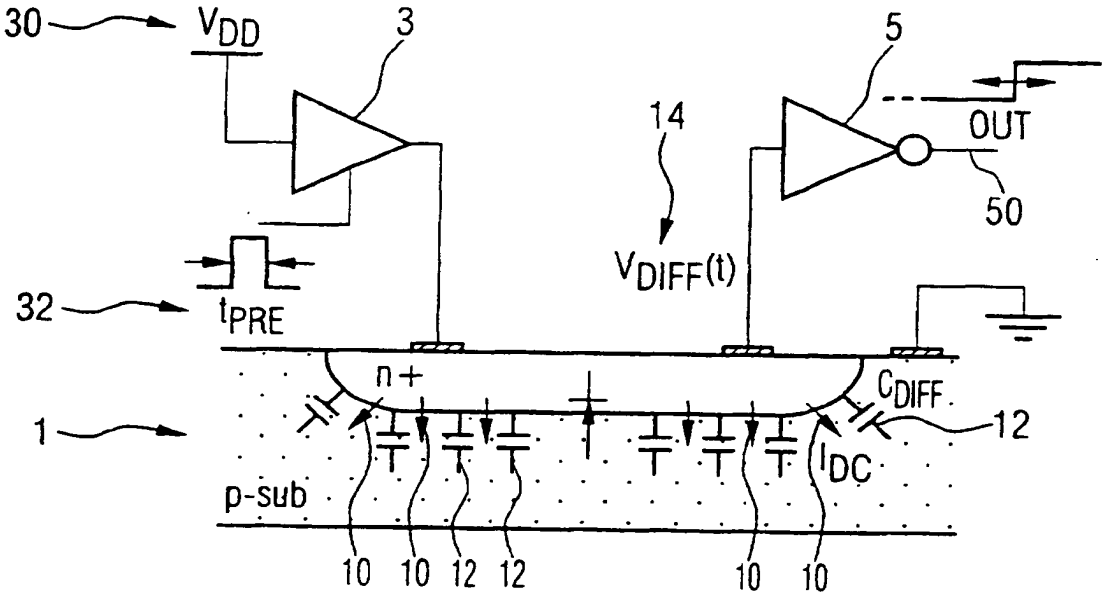


FIG 2

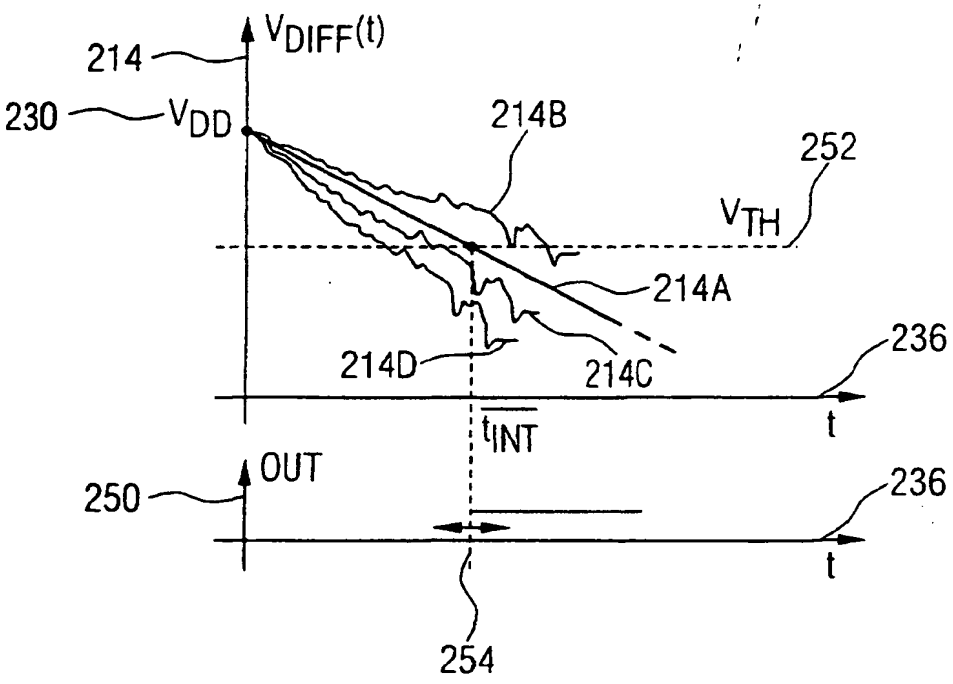


FIG 3

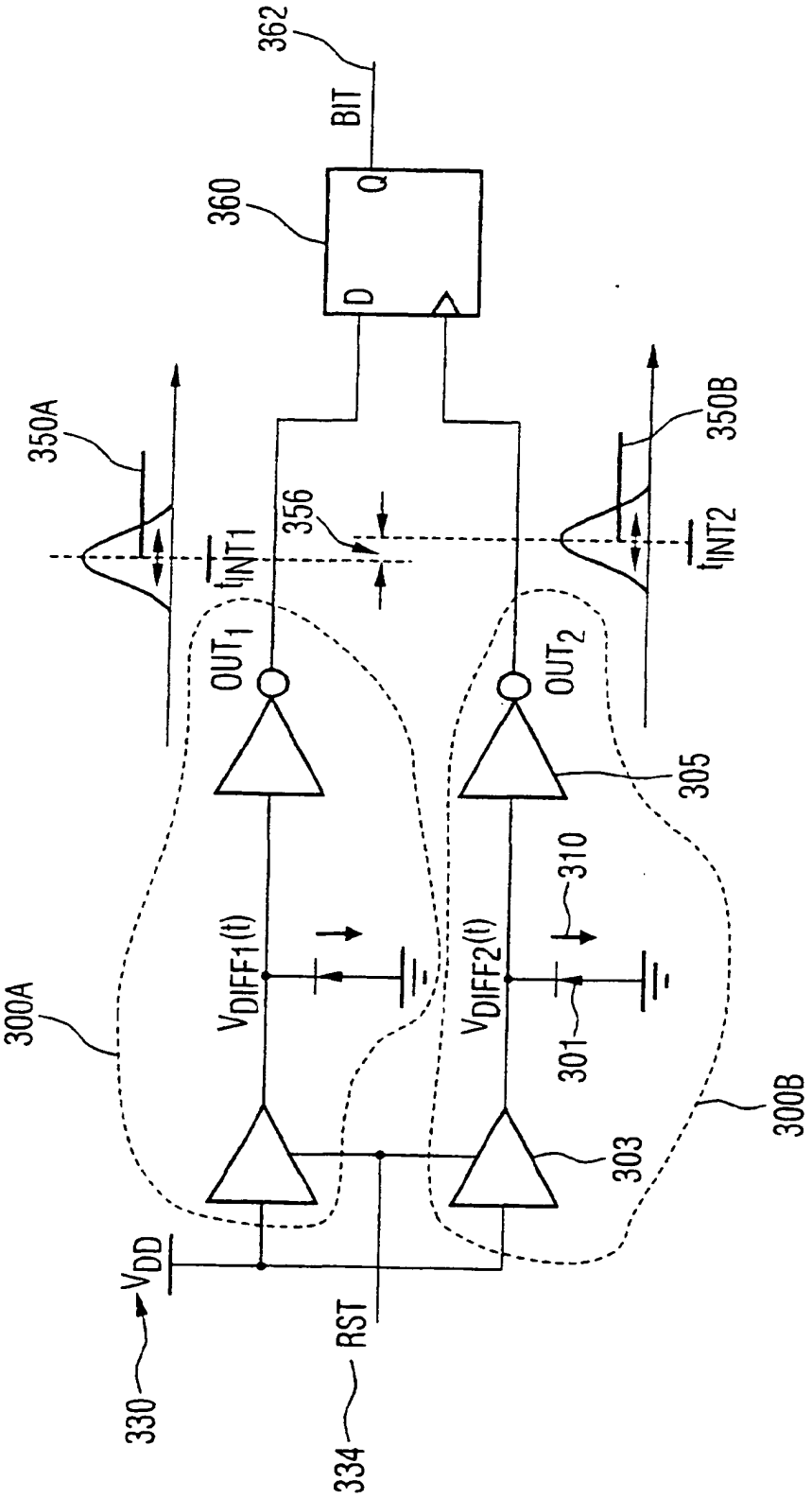


FIG 4

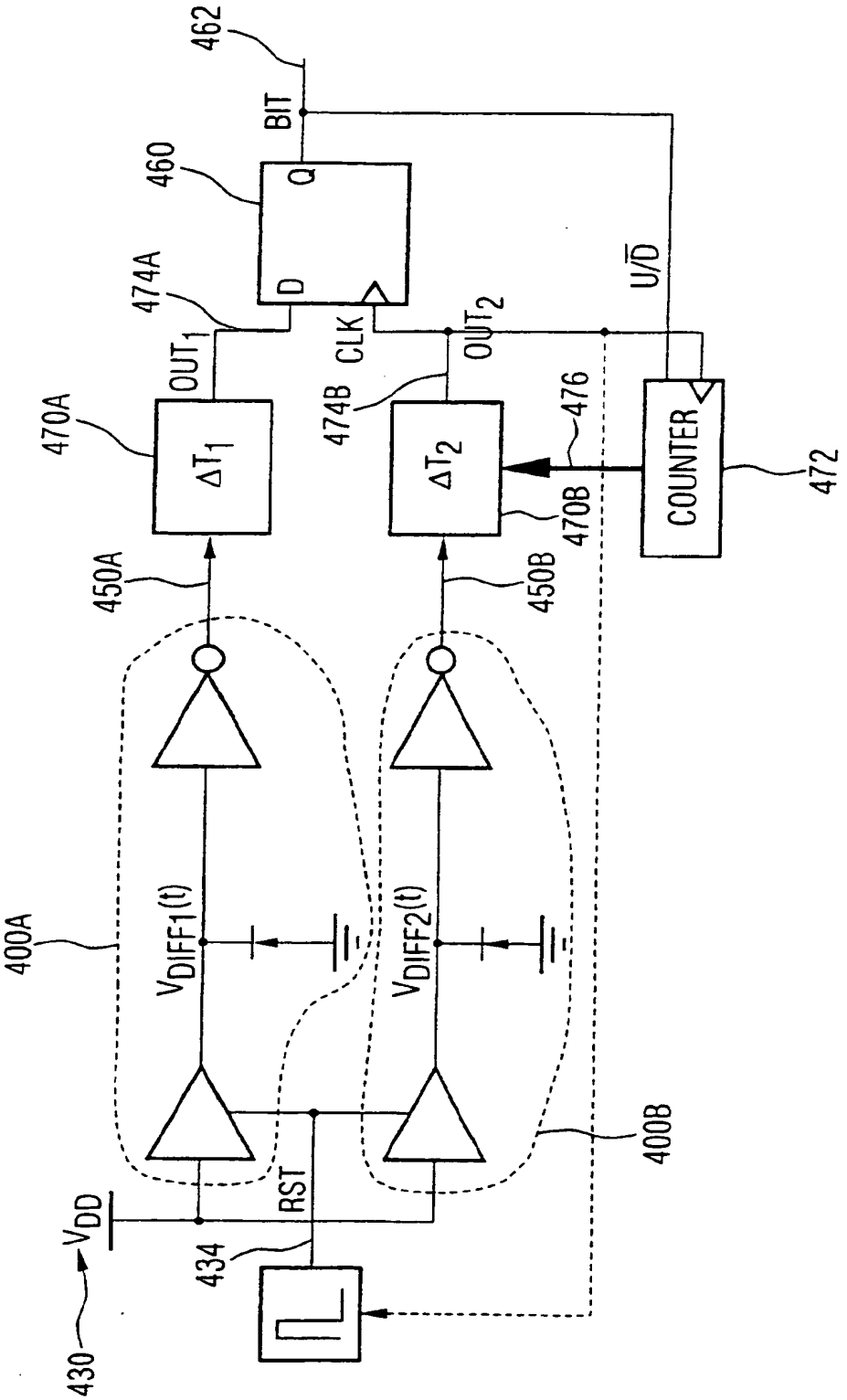


FIG 5

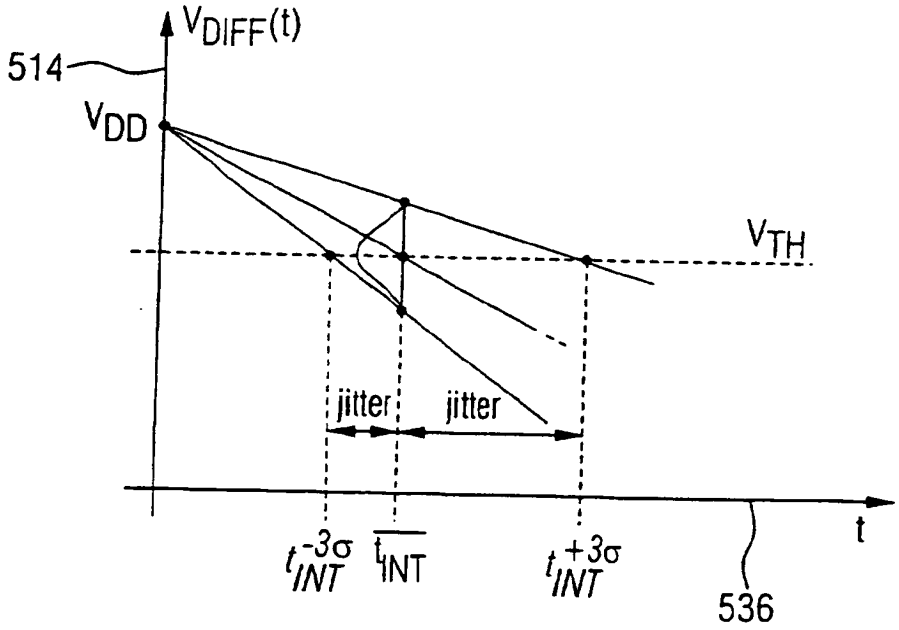
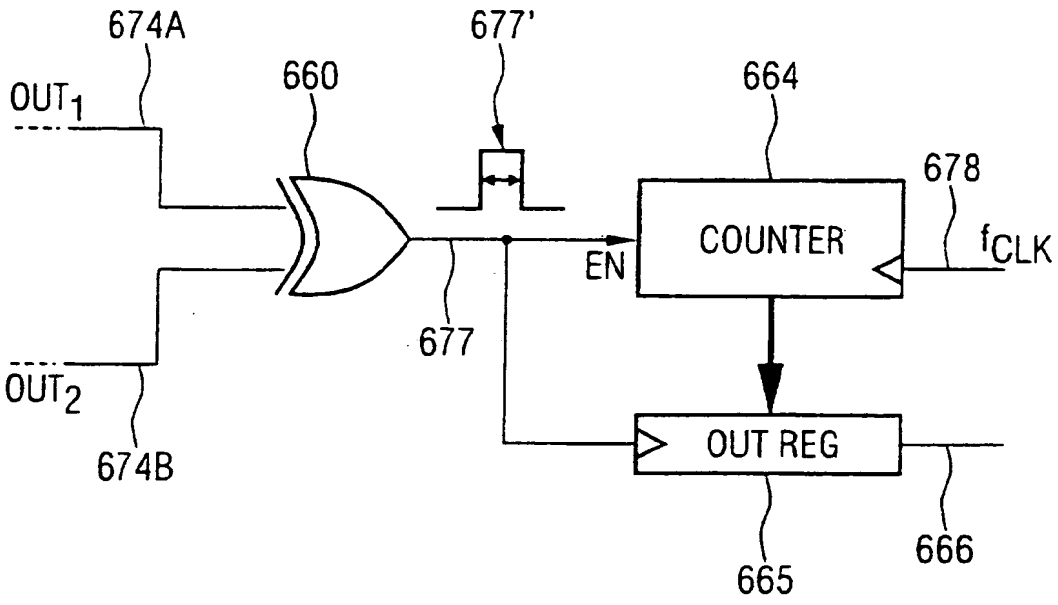


FIG 6



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 02 0077

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	EP 0 981 081 A (JAPAN SCIENCE & TECH CORP ;SYSTEM IND LAB CO LTD (JP)) 23 February 2000 (2000-02-23) * abstract; figures 1,2 *		G06F7/58
A	US 4 853 884 A (BROWN DANIEL P ET AL) 1 August 1989 (1989-08-01) * abstract; figure 1 *		
D,A	M. BUCCI, L. GERMANI, R. LUZZI, A. TRIFILETTI, M. VARANONUOVO: "A High-Speed Oscillator-Based Truly Random Number SOurce for Cryptogrphic Applications on a Smart Card IC" IEEE TRANSACTIONS ON COMPUTERS, vol. 52, no. 4, April 2003 (2003-04), pages 403-409, XP002269732 * the whole document *		
D,A	S. PETRIE, A. CONNELLY: "A Noise-Based IC Random Number Generator for Applications in Cryptography" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, vol. 47, no. 5, May 2000 (2000-05), pages 615-621, XP002269733 * the whole document *		TECHNICAL FIELDS SEARCHED (Int.Cl.7) G06F H03K
D,A	H. TIAN, B. FOWLER, A. EL GAMAL: "Analysis of Temporal Noise in CMOS Photodiode Active Pixel Sensor" IEEE JOURNAL OF SOLID-STATE CIRCUITS, vol. 36, no. 1, January 2001 (2001-01), pages 92-101, XP002269734 * the whole document *		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	10 February 2004	Pfab, S

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 03 02 0077

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

10-02-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0981081 A	23-02-2000	JP 2000066592 A	03-03-2000
		EP 0981081 A2	23-02-2000
		US 6571263 B1	27-05-2003
US 4853884 A	01-08-1989	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

This Page Blank (uspto)

Docket # 2004P00922
Applic. #
Applicant: Franke, et al.
Lerner Greenberg Stemer LLP
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100 Fax: (954) 925-1101